SOLUTIONS

1. It follows from the assumption \( H(K|PC) = 0 \) that \( H(PK) = H(\text{PC}) = H(K|\text{PC}) = H(\text{PC}) \). For any cryptosystem, \( H(PK) = H(P) + H(K) \) holds, as the ciphertext is uniquely determined by the plaintext and the key, which are independent. From this we get

\[
H(C) + H(P|C) = H(\text{PC}) = H(PK) = H(P) + H(K).
\]

It follows that the cryptosystem achieves perfect secrecy, that is, \( H(P|C) = H(P) \), if and only if \( H(K) = H(C) \).

2. (6 pts) We compute \( 11^{-1} \mod 2008 = 1643 \) and multiply the first equation with it to get \( x \equiv 913 \mod 2008 \). We divide the second equation by three to get \( x \equiv 0 \mod 669 \). Then we use the Chinese Remainder Theorem. For that purpose we compute

\[
\begin{align*}
2008^{-1} \mod 2007 &= 1^{-1} \mod 2007 = 1 \\
669^{-1} \mod 2008 &= (3^{-1} \mod 2007)^{-1} \mod 2008 = 3(-1) \mod 2008 = 2005
\end{align*}
\]

making use of the fact that \( 2007 = -1 \mod 2008 \). Then we get

\[
x = 913 \cdot 2005 \cdot 669 + 0 \cdot 1 \cdot 2008 = 854313 \mod (669 \cdot 2008),
\]

where \( 669 \cdot 2008 = 1343352 \). Then all three solutions modulo \( 2007 \cdot 2008 \) are \( 854313 + i \cdot 1343352 \), \( i = 0, 1, 2 \), that is, \( x = 854313, 2197665 \) and \( 3541017 \).

3. (a) We check that the irreducible polynomial \( f(x) = x^3 + x^2 + 1 \) does not divide the polynomial \( g(x) = x^4 + x^3 + x^2 + 1 \). Then we can calculate \( \text{lcm}(f(x), g(x)) = f(x)g(x) = x^7 + 1 \).

(b) By Theorem 2 (Lecture 4) all sum sequences \( S_1 + S_2 \) can be generated using polynomial \( x^7 + 1 \), which clearly has exponent 7. By Theorem 3 the period of the sum sequence divide 7. Hence 7 is the largest possible period.

4. We make the table

<table>
<thead>
<tr>
<th>( x_1 )</th>
<th>( x_2 )</th>
<th>( x_3 )</th>
<th>( y_1 )</th>
<th>( y_2 )</th>
<th>( x_1 \oplus x_2 \oplus y_1 )</th>
<th>( x_1 \oplus x_2 \oplus y_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Then calculating the biases we get

$$\Pr[x_1 \oplus x_2 \oplus y_1 = 0] - \frac{1}{2} = \frac{4}{8} - \frac{1}{2} = 0$$ and

$$\Pr[x_1 \oplus x_2 \oplus y_2 = 0] - \frac{1}{2} = \frac{6}{8} - \frac{1}{2} = \frac{1}{4} \neq 0.$$ 

The correct reply is: $y_2$. 
